CLAIMS

The invention claimed is:

1. A method for authenticating an identity of an individual, comprising the steps of:

receiving a personal identification number (PIN) and a social security number (SSN) of an individual; and

authenticating an identity of the individual when the received PIN and the received SSN correspond to a registered PIN and a registered SSN of the individual.

2. The method of claim 1, further comprising the step of:

registering the PIN of the individual with the SSN of the individual through a registration provider.

3. The method of claim 2, wherein the registration provider includes banks and savings and loan associations.

4. The method of claim 2, wherein the step of registering the PIN of the individual with the SSN of the individual through a registration provider includes the step of:

verifying an identity of the individual before providing the individual with access to a secure terminal for inputting the PIN and the SSN.

5. The method of claim 4, wherein the identity of the individual is verified by an employee of the registration provider through examination of at least one of a drivers license, a passport, an SSN card, a credit card and a birth certificate.

6. The method of claim 2, further including the steps of:

monitoring authentication requests for the individual;

flagging the individual when the number of failed authentication requests are above a predetermined level during a predetermined period; and

notifying at least one of the registration provider and the individual of a potential identity theft when the associated authentication requests are above the predetermined level during the predetermined period.

7. The method of claim 4, wherein the secure terminal is connected to an entity computer system that is in communication with a service provider computer system, and wherein the service provider computer system accesses a secure database to determine whether the entered PIN and the entered SSN correspond to a registered PIN and a registered SSN of the individual.

8. The method of claim 1, wherein the PIN includes one of numerals, characters and a combination of numerals and characters.

9. A system for authenticating an identity of an individual, comprising:

a service provider computer system in communication with an entity computer system, the service provider computer system storing code that when executed by the service provider computer system instructs the service provider computer system to perform the steps of:

receiving a personal identification number (PIN) and a social security number (SSN) of an individual from the entity computer system; and

authenticating an identity of the individual by sending an individual identity authentication message to the entity computer system when the received PIN and the received SSN correspond to a registered PIN and a registered SSN of the individual.

10. The system of claim 9, wherein the service provider computer system includes additional code for instructing the service provider computer system to perform the additional step of:

registering the PIN of the individual with the SSN of the individual through a registration provider.

11. The system of claim 10, wherein the registration provider includes banks and savings and loan associations.

12. The system of claim 10, wherein the step of registering the PIN of the individual with the SSN of the individual through a registration provider only occurs after the registration provider verifies the identity of the individual.

13. The system of claim 12, wherein the identity of the individual is verified by an employee of the registration provider through examination of at least one of a drivers license, a passport, an SSN card, a credit card and a birth certificate.

14. The system of claim 10, wherein the service provider computer system includes additional code for instructing the service provider computer system to perform the additional steps of:

monitoring authentication requests for the individual;

flagging the individual when the number of failed authentication requests are above a predetermined level during a predetermined period; and

notifying at least one of the registration provider and the individual of a potential identity theft when the associated authentication requests are above the predetermined level during the predetermined period.

15. The system of claim 9, wherein the service provider computer system accesses a secure database to determine whether the received PIN and the received SSN correspond to a registered PIN and a registered SSN of the individual.

16. The system of claim 9, wherein the PIN includes one of numerals, characters and a combination of numerals and characters.

17. A system for authenticating an identity of an individual, comprising:

a service provider computer system in communication with an entity computer system, the service provider computer system storing code that when executed by the service provider computer system instructs the service provider computer system to perform the steps of:

registering a personal identification number (PIN) of an individual with a social security number (SSN) of the individual through a registration provider.

receiving the PIN and the SSN of the individual from the entity computer system; and

authenticating an identity of the individual by sending an individual identity authentication message to the entity computer system when the received PIN and the received SSN correspond to a registered PIN and a registered SSN of the individual.

18. The system of claim 17, wherein the registration provider includes banks and savings and loan associations.

19. The system of claim 17, wherein the service provider computer system includes additional code for instructing the service provider computer system to perform the additional steps of:

monitoring authentication requests for the individual;

flagging the individual when the number of failed authentication requests are above a predetermined level during a predetermined period; and

notifying at least one of the registration provider and the individual of a potential identity theft when the associated authentication requests are above the predetermined level during the predetermined period.

20. The system of claim 17, wherein the service provider computer system accesses a secure database to determine whether the entered PIN and the entered SSN correspond to a registered PIN and a registered SSN of the individual.

21. The system of claim 17, wherein the PIN includes one of numerals, characters and a combination of numerals and characters.